

## APPLE (iPhone) ဖုန်းများကို စစ်ဆေးခြင်း (လိုတိုရှင်း)

### ဖုန်းထဲမှ အချက်အလက်များကို ရယူခြင်း (Acquisition) နည်းလမ်းများ

#### Manual Acquisition

Manual Acquisition နည်းလမ်းကတော့ အလွယ်ဆုံးနည်းလမ်းဖြစ်ပါတယ်။ ဥပမာ ကောင်မလေးက ကောင်ကလေးရဲ့ ဖုန်းကိုယူစစ်သလိုမျိုးဖြစ်ပါတယ်။ ဒါကအလွယ်တစ်ကူ စစ်ဆေးနိုင်သလို တစ်ဖက်ကလဲ အလွယ်တကူ Evidence သိုဝှက်ထားတာတွေကို ဖျောက်ဖျက်တာတွေပြုလုပ်နိုင်ပါတယ်။

ဥပမာ။ Messenger ဆိုရင် Archive လုပ်ပြီး Chat List ကိုဖျောက်ထားသလိုပေါ့။ 😊

ပြည်ပမှာရော ဒီလို Manual နည်းနဲ့စစ်လားဆိုရင် စစ်ဆေးပါတယ်။ ဥပမာ Mobile Forensics Tools မှာ Camera တပ်ပြီး ဖုန်းမှာရှိတဲ့ အချက်အလက်တွေကို ရိုက်ယူတာ ဖြစ်ပါတယ်။

#### Logical Acquisition

Logical Acquisition နည်းလမ်းကတော့ ဖုန်းက Unlock ဖြစ်နေတဲ့ အချိန်။ ဖုန်းရဲ့ Passcode ကိုသိနေတဲ့ အချိန်မှာပြုလုပ်တာဖြစ်ပါတယ်။ လက်ရှိစာရေးတဲ့ အချိန်မှာ Apple Phone တွေကို Acquisition လုပ်ရာမှာ Logical နည်းလမ်းက အသုံးအပြုဆုံး နည်းလမ်းဖြစ်ပါတယ်။ Apple Device တွေမှာပါတဲ့ Apple File Connection (AFC)

Protocol ကိုအသုံးပြုပါတယ်။ AFC ကို မသုံးပဲ iTunes Backup ယူပြီး iTunes သုံးပြီး ကြည့်ရင်လဲ အတူတူပါပဲ။

Logical Acquisition နည်းလမ်းမှာ အားနည်းချက်က လက်ရှိဖုန်းထဲမှာ ရှိတဲ့ Information တွေကိုပဲရယူနိုင်ပြီး အရင်ကသုံးခဲ့တဲ့ အချက်အလက်တွေ System Information တွေကိုမရယူနိုင်ပါဘူး။ အရှင်းလင်းဆုံးပြောရရင် File System ရဲ့ အချက်အလက်တွေနဲ့ Deleted Data တွေကိုမရယူနိုင်တာပါ။ Apple Developer တွေကလဲ အချို့အချက် အလက်တွေကို Logical Acquisition ပြုလုပ်ရာမှာမပါ သွားအောင် ကန့်သတ်ထား တတ်ပါတယ်။

### **File System Acquisition**

File System Acquisition နည်းလမ်းကိုတော့ Apple Device က Jailbreak ဖြစ်နေတဲ့ အခါ။ ဒါမှမဟုတ် File System Information ကိုရယူရမဲ့ အခြေအနေဖြစ်တဲ့ အချိန်မှာ ပြုလုပ်တာဖြစ်ပါတယ်။ File System ကိုရယူမယ်ဆိုရင် Phone က Jailbreak မပြုလုပ်ထားရင် (ဖုန်းကို Jailbreak ပြုလုပ်ရပါတယ်။)

Apple ရဲ့ အချို့သော အားနည်းချက်တွေကြောင့် Jailbreak မလုပ်ပဲ File System ကို ရယူနိုင်တဲ့ Apple ဖုန်းတွေရှိပါတယ်။ ဒါပေမဲ့ Apple က အခု iOS Version မှာ အားနည်းချက်တွေကို ပြင်လိုက်တဲ့အတွက် ဖုန်းမှာ အားနည်းချက်ရှိပေမဲ့ iOS Update လုပ်ထားရင် မရနိုင်တော့ပါ။

File System Acquisition ပြုလုပ်တဲ့အခါမှာ ရရှိတဲ့ Data က Logical Acquisition ပြုလုပ်တဲ့အချိန်မှာ ရရှိတဲ့ Data တွေအတိုင်းရရှိပါတယ်။ ဒါပေမဲ့ File System အချက်အလက်တွေအပြင် Database File အချို့ပါရရှိပါတယ်။ အများဆုံး SQLite File တွေရရှိပါတယ်။ အဲဒီကနေ Logical မှာမရတဲ့ အချက်အလက်တွေကို ရနိုင်ပါတယ်။

ဥပမာ ဒီဖုန်းထဲကို အခု Sim card မထည့်ခင်က ဘယ် Sim Card ထည့်ထားတယ် ဘယ်နံပါတ်လဲဆိုတာမျိုးတွေ ရရှိနိုင်ပါတယ်။

## Physical Acquisition

Physical Acquisition နည်းလမ်းကတော့ အခုစာရေးတဲ့အချိန်အထိ Iphone 5c အထိသာရရှိပါတယ်။ Physical Acquisition လုပ်ရင်တော့ ဖျက်ထားတဲ့ Data တွေထဲကမှ Overwrite ဖြစ်မသွားတဲ့ Data တွေကိုရရှိနိုင်ပါတယ်။ Iphone 5c အထိပဲရတဲ့အတွက် ခန့်မှန်းထားတာကောင်းပါတယ်။

## Pattern Of Life

Logical Acquisition ဒါမှမဟုတ် File System Acquisition ဘယ်လိုနည်းလမ်းနဲ့ ရယူနိုင်သည် ဖြစ်စေ။ Pattern Of Life ကတော့ စစ်ဆေးရာမှာ အရေးကြီးဆုံးဖြစ်ပါတယ်။ Pattern Of Life ဆိုတာက

- User က ဘယ်လို လူမျိုးလဲ
- အခု ဖုန်းကို ဘာအတွက်ကြောင့်သူ သုံးတာလဲ
- ဖုန်းထဲက ဘယ်အရာတွေကို အသုံးအများဆုံးလဲ
- ဘယ်သူတွေနဲ့ ဆက်သွယ်သလဲ
- အများဆုံးဘယ်သူနဲ့ဆက်သွယ်သလဲ

Pattern Of Life ကိုစစ်ဆေးနိုင်ဖို့အတွက် Full File System ကို ရယူနိုင်ရင် အကောင်းဆုံးဖြစ်ပါတယ်။ စစ်ဆေးသူကလဲ Apple File System အကြောင်းကို နားလည် ထားရင် အကောင်းဆုံးဖြစ်ပါတယ်။ ဒါမှ ဘယ်လို Artifacts အချက်အလက်ကိုလို ချင်တယ်။ အဲဒီအချက်အလက်က ဘယ်မှာရှိတယ်ဆိုတာကို သိနိုင်မှာ ဖြစ်ပါတယ်။

အခုပုံမှာပါတာက ပထမပုံက Logical Acquisition နည်းလမ်းနဲ့ရယူထားတာ ဖြစ်ပါတယ်။ ဒုတိယပုံက File System ကိုရယူထားတာဖြစ်ပါတယ်။ ဒုတိယပုံမှာ File System ကိုရယူထားတာဖြစ်တာကြောင့် Device ကို ဘယ်အချိန်မှာ Lock - Unlock လုပ်တယ်ဆိုတာကိုတွေ့နိုင်ပါတယ်။

| Data                   |     |                   |
|------------------------|-----|-------------------|
| Calendar               | 21  | Call Log          |
| Contacts               | 9   | Chats             |
| Installed Applications | 373 | Cookies           |
| Notes                  | 1   | Device Locations  |
| Web Bookmarks          | 10  | Instant Messages  |
|                        |     | Log Entries       |
|                        |     | Searched Items    |
|                        |     | User Accounts     |
|                        |     | Web History       |
|                        |     | Wireless Networks |
| Data Files             |     |                   |
| Archives               | 2   | Configurations    |
| Images                 | 51  | Databases         |
| Videos                 | 1   | Text              |
|                        |     | Uncategorized     |

## Logical Acquisition

|                                     |     |                           |                           |                    |            |
|-------------------------------------|-----|---------------------------|---------------------------|--------------------|------------|
| <input checked="" type="checkbox"/> | 108 | 31-Jan-19 13:57:20(UTC+0) | 31-Jan-19 13:57:32(UTC+0) | Display On/Off     | Display on |
| <input checked="" type="checkbox"/> | 109 | 31-Jan-19 13:57:32(UTC+0) | 31-Jan-19 13:57:36(UTC+0) | Display On/Off     | Display on |
| <input checked="" type="checkbox"/> | 110 | 03-Feb-19 06:31:48(UTC+0) | 03-Feb-19 06:27:20(UTC+0) | Device Lock Status | Unlocked   |
| <input checked="" type="checkbox"/> | 111 | 03-Feb-19 06:38:52(UTC+0) | 03-Feb-19 06:42:52(UTC+0) | Audio Output Route | Speaker    |
| <input checked="" type="checkbox"/> | 112 | 03-Feb-19 06:43:00(UTC+0) | 03-Feb-19 06:43:28(UTC+0) | Display On/Off     | Display on |
| <input checked="" type="checkbox"/> | 113 | 03-Feb-19 06:43:08(UTC+0) | 03-Feb-19 06:43:11(UTC+0) | Audio Output Route | Speaker    |
| <input checked="" type="checkbox"/> | 114 | 03-Feb-19 06:43:12(UTC+0) | 03-Feb-19 06:43:14(UTC+0) | Audio Output Route | Speaker    |
| <input checked="" type="checkbox"/> | 115 | 03-Feb-19 06:43:16(UTC+0) | 03-Feb-19 06:43:24(UTC+0) | Audio Output Route | Speaker    |
| <input checked="" type="checkbox"/> | 116 | 03-Feb-19 06:43:28(UTC+0) | 03-Feb-19 06:51:12(UTC+0) | Display On/Off     | Display on |
| <input checked="" type="checkbox"/> | 117 | 03-Feb-19 06:50:36(UTC+0) | 03-Feb-19 07:34:12(UTC+0) | Audio Output Route | Speaker    |

## File System Acquisition

အထပ်ပါ နည်းလမ်းတွေနဲ့ လုပ်လို့မရရင် Chip Off I, JTAG, ISP နည်းလမ်းတွေနဲ့ Mobile Forensics ပြုလုပ်ပါတယ်။ အဲဒီနည်းလမ်းတွေမှာလဲ ကန့်သတ်ချက် အချို့ ရှိပါတယ်။

### Mobile Forensics (Chip Off Method Limitation)

Android မှာ User တွေရဲ့ Information တွေကို လုံခြုံစွာသိမ်းထားနိုင်ဖို့နဲ့ ဖုန်းပျက်တဲ့အခါမှာ အချက်အလက်တွေကို အခြားလူကနေ အလွဲသုံးစားမလုပ်နိုင်အောင် Android Version 4 မှာ Full Disk Encryption (FDE) ကို စတင်အသုံးပြုခဲ့ပါတယ်။ Full Disk Encryption လို့ခေါ်ပေမဲ့ Flash Storage တစ်ခုလုံးကို Encryption ပြုလုပ်တာမဟုတ်ပါဘူး။ User ရဲ့ Data Partition ကိုပဲ Encryption ပြုလုပ်တာ ဖြစ်ပါတယ်။

### Full Disk Encryption (FDE)

Android Version 5 မှာ အောက်မှာဖော်ပြထားတဲ့ Feature တွေပါဝင်လာပါတယ်။

*Default, PIN, Password, Pattern, Default*

Phone က Password မရှိတဲ့ အနေအထား Factory Default လုပ်ပြီးတဲ့အနေအထား မှာဆိုရင် (Primary Key) ( AES 128-bit ) က Default Password ဖြစ်တဲ့ "default\_password" နဲ့ ပြန်ပြီး Encryption ပြုလုပ်ပါတယ်။ Mobile အမျိုးအစားပေါ် မူတည်ပြီး Default Password ကပြောင်းလဲနိုင်ပါတယ်။

User ကနေ Pin, Password ပေးတဲ့အခါမှာ Master Key (Random AES 128-bit ) က User ပေးတဲ့ Pin, Password နဲ့ ပြန်ပြီး Encryption ပြုလုပ်ပါတယ်။ User က Pin, Password အသစ်ပေးရင်လဲ Primary Key က User နောက်ထပ်ပေးတဲ့ Password ကိုပဲထပ်ပြီး Encryption လုပ်ပါတယ်။ User Data အကုန်လုံးကိုပြန်ပြီး Encryption မပြုလုပ်ပါ။

## ***Full Disk Encryption ပြုလုပ်ရင် ဘာတွေဖြစ်လာနိုင်သလဲ ?***

Phone ကို Reboot Or Power On တဲ့အချိန်တွေမှာ User Data Partition ကို Access လုပ်ဖို့အတွက် Password ရိုက်ထည့်ရပါမယ်။ မရိုက်ထည့်ရင် User Data ကို Access မလုပ်နိုင်တဲ့အတွက် Accessibility Services , Alarm, Ph Receive Call တွေပြုလုပ်လို့ရမှာမဟုတ်ပါဘူး။

### **Mobile Forensics (Chip off)**

Chip Off ပြုလုပ်တယ်ဆိုတာ Phone မှာ Pin, Password ခံထားတယ်။ Pin, Password ကို Remove လုပ်ဖို့ Phone မှာ ဘာအားနည်းချက်မှ လဲမရှိဘူး။ Mobile Forensics Tools ကလဲ မလုပ်နိုင်တဲ့အခါမှာ Phone ရဲ့ Flash Storage ကို ဖြုတ်ပြီး Chip Reader ပေါ်မှာ Chip ကိုတင်ပြီး Chip ထဲက Data ကိုရယူတာဖြစ်ပါတယ်။ Full Disk Encryption ပြုလုပ်ထားရင် Flash Storage ကိုဖြုတ်ပြီး ဖတ်ရင်လဲ Encryption လုပ်ထားတဲ့ Key (User ပေးထားတဲ့ Pin Password) ကို မသိရင် Chip ထဲ Data တွေကိုဖတ်လို့မရပါဘူး။

**Android-9** နဲ့ သူရဲ့အောက် Version တွေပဲ Full Disk Encryption ကိုအသုံးပြုနိုင်ပါတယ်။ **Android-10** အထက် Version တွေကတော့ File-Based Encryption ကိုပဲအသုံးပြုပါတယ်။

**Android 10-12** ကြားမှာလဲ Android Version အနိမ့်ကနေ **Android 10-12** ကို Update လုပ်ထားရင် Full-Disk Encryption ကို Support ပြုလုပ်ပါတယ်။ ဥပမာ Android Version 10 ကနေ 11 ကို Update ပေးလိုက်တဲ့အချိန်မျိုးမှာ ဖြစ်ပါတယ်။

**Android-13** မှာတော့ Full Disk Encryption ကို အသုံးပြုလို့မရတော့ပါ။ File-Based Encryption ကိုပဲ အသုံးပြုပါတယ်။ ဒါဆိုရင် Password မသိလို့ Chip Off

လုပ်ပါတယ်ဆိုမှ Password ကပြန်လိုလာပြန်တယ်။ ဒါဆိုရင် Chip Reader ကနေရလာတဲ့ .bin File ကို Offline Attack (Password Attacks) ပြုလုပ်တဲ့နည်း ဖြစ်ပါတယ်။ Pin, Or Password ကလဲ 4 လုံးလား 4 လုံးအထက်လား။ 😞 But Difficult and Need Skillful.....

### **File-Base Encryption (FBE)**

Android Version-7 မှာ File-Base Encryption (FBE) ကိုစတင်အသုံးပြု လာပါတယ်။ Full Disk Encryption (FDE) မှာ User Data ကို Encryption လုပ်ထားတဲ့အတွက် User ကနေ Password ရိုက်မှသာ User Data Partition ထဲမှာရှိတဲ့ Application တွေ Data တွေကို အသုံးပြုလို့ရမှာ ဖြစ်ပါတယ်။

**Android Version -7** မှာ Direct Boot Mode ပါဝင်လာတဲ့အတွက် Password မရိုက်ခင်မှာ အချို့သော Application တွေကိုသုံးလို့ရအောင်ပြုလုပ်ပေးထားပါတယ်။ ဥပမာ Schedule, Alarm, SMS, Call Log Notification, Etc ..

Mobile Phone Model တွေ အပေါ်မူတည်ပြီး အစကတည်းက သတ်မှတ်ပေးထား တာရှိသလို Direct Boot Mode မှာ ကိုယ်ပေါ်စေချင်တာကို ကိုယ်တိုင်သတ်မှတ် ပေးလို့ လဲရပါတယ်။ အခုလို Direct Boot Mode အသုံးပြုလို့ရအောင် Android မှာ Storage Partition (2) ခု ပါဝင်လာပါတယ်။

### **Credential Encrypted Storage (CE Storage)**

User Data Partition ဖြစ်ပြီး User ကနေ Pin, Password ရိုက်ထည့်မှသာ Partition ကို Fully Access ရမှာဖြစ်ပါတယ်။

### **Device Encrypted Storage (DE Storage)**

Direct Boot Mode မှာရော User ကနေ Pin, Password ရိုက်ပြီးတဲ့ အချိန်မှာပါ (2) မျိုးလုံးအသုံးပြုနိုင်ပါတယ်။



Direct Boot Mode မှာ Application တစ်ခုက Data အသုံးပြုဖို့လိုအပ်လာတယ် ဆိုရင် Device Encrypted Storage (DE Storage) ထဲကနေ Data ကိုယူသုံး မှာဖြစ်ပါတယ်။ ဒါကြောင့် Mobile Phone အမျိုးအစား အပေါ်မူတည်ပြီး Default သတ်မှတ်ထားတာရှိသလို ကိုယ်အသုံးပြုလိုတာကို ကိုယ်တိုင်သတ်မှတ်ပေးရတာ ဖြစ်ပါတယ်။ (DE Storage) ကလဲ Verify Boot လုပ်တဲ့ Process အောင်မြင်ပြီးမှသာ Data ကိုယူပြီးသုံးလို့ရမှာ ဖြစ်ပါတယ်။

User Data တွေကို Access လုပ်ရမှာ (CE Storage), (DE Storage) အပေါ်မူတည်ပြီး အခုလို Key တွေခွဲထားတဲ့အတွက် Direct Boot Mode ကို File-Base Encryption (FBE) လို့ခေါ်ပါတယ်။ **Android Version 7.0–8.1** တွေမှာ File Base Encryption (FBE) က Built-in ပါတဲ့ Storage တွေမှာပဲအလုပ်လုပ်ပါတယ်။ ဖုန်းမှာ SD Card ထပ်စိုက်ထားရင် FBE က SD Card မှာ အလုပ်မလုပ်ပါဘူး။ **Android Version 9 နှင့်အထက်**မှာတော့ FBE က Phone မှာထပ်စိုက်ထားတဲ့ SD Card တွေပေါ်မှာပါ အလုပ် လုပ်ပါတယ်။

Chip Off လုပ်ရာမှာ Full Disk Encryption လို့ပဲ File Base Encryption က Credential Encrypted Storage (CE Storage) ကို Access လုပ်နိုင်ဖို့အတွက် User ပေးထားတဲ့ Pin, Password လိုပါတယ်။ Pin, Password ကို Password Attack လုပ်လို့ရနိုင်ပေမဲ့ Forensics လုပ်ဖို့အတွက် ခက်ခဲပါတယ်။ Skillful တော်တော်လေးဖြစ် မှရပါမယ်။

Apple ကတော့ Disk Encryption မှာ Android ထက်ရှေ့ပြေးပါတယ်။ 64-bit Devices တွေပေါ်လာပြီး IOS Versions 8 ကနေစပြီး Chip off ပြုလုပ်လို့မရနိုင်တော့ပါ။

Apple က 256-bit device-unique secret key (UID) ကိုအသုံးပြုထားပြီး Key ကို ဖုန်းရဲ့ Hardware ထဲမှာ သိမ်းထားပါတယ်။ (Hardware Key ဖြစ်ပြီး Key ကို အခြားသော Tools တွေနဲ့ ဖတ်လို့မရပါ။) Apple Device တစ်ခုကို UID တစ်ခုဖြစ်ပါတယ်။ UID ကိုပဲ



User ပေးထားတဲ့ Passcode နဲ့ ထပ်ပြီး Encryption ပြုလုပ်ထားပြီး ရလာတဲ့ (Passcode Key) နဲ့ Data ကို Secure ဖြစ်အောင်ပြုလုပ်ထားပါတယ်။ ပိုပြီးလုံခြုံအောင် Class Key, File System Key တွေနဲ့ ထပ်ပြီး Encryption ပြုလုပ်ထားပါသေးတယ်။ UID Key ကို Apple ကလွဲပြီး အခြား Hardware, Software တွေနဲ့ ဖတ်လို့မရနိုင်ပါ။ Apple လိုပဲ Chip off လုပ်လို့မရနိုင်တဲ့ Phone နောက်တစ်ခုက Blackberry ပဲဖြစ်ပါတယ်။

Full Disk Encryption, File Base Encryption တွေကြောင့် Joint Test Access Group (JTAG) ပြုလုပ်ရမှလဲ ရလာတဲ့ .Bin File (Raw User Data File) ကိုဖြည့်ကြည့်ဖို့အတွက် User ပေးထားတဲ့ Pin, Password တွေလိုလာပါတယ်။



**Removing Chip**



**Example Chip Reader**

**Aung Zaw Myo**

[www.forensicsmyanmar.com](http://www.forensicsmyanmar.com)